CLAIMS

1. A method for generating an FPGA bitstream having bits representing configuration of the FPGA and bits controlling loading of the bitstream, comprising:

generating an unencrypted bitstream including both the bits representing the configuration of the FPGA and the bits controlling loading of the bitstream; and

encrypting the bits representing the configuration of the FPGA using at least one key; and

combining the bits controlling loading of the bitstream with the encrypted bits representing the configuration of the FPGA to produce a partially encrypted bitstream.

2. The method of Claim 1 further comprising:

loading the partially encrypted bitstream into the FPGA;

decrypting the partially encrypted bitstream within the FPGA using the key; and

configuring the FPGA using the decrypted bitstream.

3. The method of Claim 2 wherein the key for decrypting the bits representing the configuration of the FPGA is stored in the FPGA.

4. The method of Claim 3 wherein the key in the FPGA is stored in volatile memory that may be powered by a battery.

5. The method of Claim 3 wherein the key in the FPGA is stored in nonvolatile memory.

6. The method of Claim 1 wherein some bits controlling loading of the bitstream provide an indication that the bits representing configuration of the FPGA are encrypted.

7. A method for generating an FPGA bitstream having bits representing configuration of the FPGA and bits controlling loading of the bitstream, comprising:

providing an indication as to whether the bits representing configuration of the FPGA are to be encrypted;

generating an unencrypted bitstream including both the bits representing the configuration of the FPGA and the bits controlling loading of the bitstream; and

if the indication indicates that the bits representing configuration of the FPGA are to be encrypted, encrypting the bits representing the configuration of the FPGA.